UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/795,776	03/08/2004	David P. Johnson	RSW920030219US1	4089

23307 7590 08/22/2007

SYNNESTVEDT & LECHNER, LLP
1101 MARKET STREET
26TH FLOOR
PHILADELPHIA, PA 19107-2950

EXAMINER	
PICH, PONNOREAY	
ART UNIT	**PAPER NUMBER**
2135	

MAIL DATE	DELIVERY MODE
08/22/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/795,776	JOHNSON ET AL.	
	Examiner	Art Unit	
	Ponnoreay Pich	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 March 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-21* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *3/04*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claims 1-21 are pending.

Information Disclosure Statement

The IDS submitted on 3/8/04 has been considered.

Claim Objections

Claims 2-3, 9-10, 12, 16-17, and 19 are objected to because of the following informalities:

1. Claims 2, 9, and 16 refer to "the software solution". Since "said software solution" is used elsewhere, the examiner respectfully suggests maintaining consistency between usage of "said" and "the" and change "the software solution" in claims 2, 9, and 16 to "said software solution".
2. Claims 3, 10, and 17 recites "interface", which the examiner assumes should be "interfaces".
3. Claim 12 refer to "correction method", which the examiner assumes should be "correction system".
4. Claim 19 refers to "correction method", which the examiner assumes should be "correction computer program product".
5. Appropriate correction is required.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 8-14 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claim 8 is directed towards a system comprising means for analyzing, means for attempting access, and means for storing. It is assumed that 112, 6th paragraph is being invoked via use of means plus function language—confirmation by applicant is respectfully requested.

It would appear that the means for analyzing and means for attempting access are disclosed in the specification as the VAF tool 102. Applicant's specification further states in paragraph 31 that instructions executed on a processor creates means for implementing the functions of discussed. It would appear then that the VAF tool, being instructions executed by a processor, is software per se. Likewise, the means for storing, which the specification discloses as being database 110 is also software per se since it is implemented by instructions executed by a processor.

Because claim 8 appears to be directed solely towards instructions executed by a processor, claim 8 is not statutory since it is directed towards software per se. Applicant can overcome this rejection by reciting some form of hardware as part of the system of claim 8. Claims 9-14 are dependent on claim 8 and also do not appear to recite any hardware as part of the claimed system and as such are also not statutory since the claims are directed towards software per se.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1, 8, and 15 are rejected under 35 U.S.C. 102(a/e) as being anticipated by Reshef et al (US 2003/0233581).

Claims 1, 8, and 15:

As per claim 1, Reshef discloses:

1. Analyzing a software solution, i.e. application, to identify legal and illegal external interfaces thereto (paragraphs 23-25, 34, 55, 67, and 97). *The cited paragraphs discuss how Reshef's invention analyzes an application to identify the application's interfaces with external clients. The identified interfaces are further analyzed to identify any possible vulnerabilities, i.e. illegal external interfaces, which may be used to access the application via mutated requests.*
2. Attempting to access said software solution using the identified illegal external interfaces (paragraphs 10, 25, and 37). *The cited sections discuss how Reshef's invention attempts to access the application using possible illegal external interfaces via mutated requests.*

3. Storing a record of any illegal external interfaces that allow access to said software solution (paragraphs 26-27 and 35). *Note that a record of successful attacks is stored in database 18. These successful attacks are indication of illegal external interfaces that allow access to the application.*

Claims 8 and 15 recite limitations substantially similar to what is recited in claim 1 and are rejected for similar reasons. The difference between the claims is that claim 8 is directed towards a system comprising means to perform the method of claim 1 while claim 15 is directed towards a computer program product comprising computer-readable storage medium having computer-readable program code to perform the method of claim 1.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 2, 9, and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Reshef et al (US 2003/0233581) in view of applicant's admittance of prior art, herein referred to as AAPA.

Claims 2, 9, and 16:

Reshef does not explicitly disclose wherein said software solution comprises at least two independent software programs interacting to form said software solution. However, AAPA discloses that it was well known for software solutions to comprise at least two independent software programs interacting to form said software solution (specification: paragraph 2).

At the time applicant's invention was made, it would have been obvious to one of ordinary skill in the art to utilize Reshef's invention to secure a software solution which comprises at least two independent software programs interacting to form said software solution. One skilled would have been motivated to do so because Reshef recognizes that securing vulnerabilities at the network level is insufficient and there also exists a need to ensure security at the application level (paragraphs 6-7). Using Reshef with the prior art software solution would provide an automated way of ensuring application level security and would provide an organization with a repeatable and potentially cost-effective process for conducting application/software security audits (paragraph 27).

Claims 3-5, 10-12, and 17-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Reshef et al (US 2003/0233581) in view of Neelay et al (US 2004/0064722).

Claims 3, 10, and 17:

Reshef does not explicitly disclose automatically deploying a corrective measure to said software solution based upon said identified illegal external interface. However,

after Reshef's invention performs its analysis, a report is generated for purposes of recommending fixes for vulnerabilities, i.e. identified illegal external interfaces, discovered (paragraph 27). Further, Neelay discloses of an automated system of deploying corrective measures that neutralizes vulnerabilities (paragraph 20).

The examiner asserts that a person of ordinary skill with respect to the present application is someone with at least a Bachelor of Science degree with a focus in security or someone with equivalent industry experience. Based on Neelay's further teachings, it would have been obvious to one of ordinary skill in the art to modify Reshef's invention such that it automatically deployed corrective measures to the software solution based on identified illegal external interfaces. One skilled would have been motivated to do so because automatically deploying corrective measures would promote security since any delays in application of the corrective measure is a window of opportunity for an attack against the software solution which may succeed.

The claimed invention is also not patentable because the incorporation of Neelay's teachings of automated patching to Reshef's known invention, which is ready for improvement, yields a predictable result. Note that Neelay discloses that after identifying vulnerability in a computer's software, manual installation of corrective measures could result in unnecessary delays. Based on Reshef's teachings alone, one skilled should appreciate that Reshef's invention is an invention which is ready for improvement since he does not discuss in what manner the discovered vulnerabilities are dealt with. Incorporating Neelay's teachings of automated patching for vulnerabilities to Reshef's invention would yield a predictable result of an system which

automatically scans applications for vulnerabilities, such as illegal external interfaces, and automatically patch those vulnerabilities.

Claims 4, 11, and 18:

Reshef further discloses storing each of said corrective measures in a memory (paragraph 27). The report 402 provided by Reshef's invention suggests corrective measures, i.e. fixes. Writing these corrective measures to a report reads on storing the corrective measures in a memory.

Note that Neelay also discloses the limitation (paragraph 27). The installation of the patches to fix detected vulnerabilities means that the corrective measures were written to a memory, i.e. stored to memory.

Claims 5, 12, and 20:

Reshef implicitly discloses making said stored record of illegal external interfaces that allow access available to all users of said detection and correction method/system/computer program product (paragraphs 27 and 69). In the cited paragraphs, Reshef discloses that public databases that publish known vulnerabilities that anyone can access were well known in the art at the time applicant's invention was made. The purpose of such databases was so that other users with similar systems could learn about new vulnerabilities that someone else may have discovered and take appropriate actions against the vulnerabilities. Since Reshef's invention generates a report of illegal external interfaces that allow access to an application, one skilled would expect that at the time applicant's invention was made, the public databases would be

utilized to alert other users with similar software solutions of any new vulnerabilities discovered using Reshef's invention.

Reshef does not explicitly disclose making said stored record of corrective measures available to all users of said detection and correction method/system/computer program product. However, the limitation is obvious over Neelay's teachings of providing a server from which patches for software vulnerabilities could be downloaded (paragraphs 8 and 23). From this teaching, it would have been obvious to one of ordinary skill in the art to make stored record of corrective measures available to users of Reshef's modified invention globally.

At the time applicant's invention was made, it would have been obvious to one of ordinary skill in the art to further modify Reshef's invention such that the stored record of illegal external interfaces that allow access and the stored record of corrective measures were available to all users globally. One skilled would have been motivated to do so because making such information available to other global users would increase the chance that other users become aware of newly discovered problems and patch their systems.

Claims 7, 14, and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Reshef et al (US 2003/0233581) in view of Cedar et al (US 2003/0236994).

Claims 7, 14, and 21:

Reshef further discloses mapping each legal and illegal external interface into a machine-readable format (paragraphs 35-37). Note that in Reshef's invention, automated analysis of the application is preformed whereby Reshef's invention discovers legal and illegal external interfaces into the application. This information is then used to by attack engine 22 to attack the interfaces to see if access is allowed. The attack engine is a software program, thus this implies that the legal and illegal external interfaces were mapped into a machine-readable format since the attack engine was able to make use of the information to try to attack the application being tested.

Reshef does not explicitly disclose analyzing an XML description of each legal and illegal external interface. However, use of XML files to store the result of security analysis was well known in the art as evidenced by Cedar (paragraph 67).

At the time applicant's invention was made, it would have been obvious to one of ordinary skill in the art to modify Reshef's invention such that after analyzing the application to discover legal and illegal external interfaces, the result was written to an XML file using XML description. As such, when the attack engine tries to attack the application, it must analyze the XML description of each legal and illegal external interface which was generated to determine how to attack the system. One skilled would have been motivated to use an XML file as database 18 as disclosed by Reshef to store the description of each legal and illegal external interface because XML is a portable data format which allows the resultant file to be viewed by many different

available public API's (Cedar: paragraph 69). This allows flexibility in the design of Reshef's attack engine since it could utilize many publicly available API's.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ponnoreay Pich whose telephone number is 571-272-7962. The examiner can normally be reached on 9:00am-4:30pm Mon-Thurs.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Ponnoreay Pich
Examiner
Art Unit 2135

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

PP